UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

KARLI NORMAND, individually and on behalf of all others similarly situated,	)	Case No.
Plaintiff,	)	CLASS ACTION
v.	)	
EMPRESS AMBULANCE SERVICES, INC., d/b/a EMPRESS EMS,	)	JURY TRIAL DEMANDED
Defendant.	)	

CLASS ACTION COMPLAINT

Plaintiff Karli Normand ("Plaintiff"), individually and on behalf of all other persons similarly situated, and through her attorneys of record, alleges the following against Defendant Empress Ambulance Services Inc., d/b/a Empress EMS ("Empress") based upon personal knowledge with respect to herself, on information and belief derived from investigation of counsel, and review of public documents as to all other matters.

INTRODUCTION

1. Empress is one of the largest, most experienced emergency and non-emergency response providers in Westchester, Rockland, Ulster, Dutchess, Putnam, and Orange Counties, and the Bronx, New York.[1] It has over 37 years of experience, focusing on providing state-of-the-art patient care by professionally trained and highly skilled personnel.[2] It also boasts a 24-hour communications center, "[h]ousing one of the most advanced computer aided systems in the region."[3]

[1] https://empressems.com/ (last visited October 6, 2022).
[2] *Id.*
[3] *Id.*

2. Plaintiff and other customers provided Empress with their Personal Health Information ("PHI") and personal identifiable information ("PII") in connection with receiving health care services from Empress. Unfortunately for Plaintiff, Empress did not adequately safeguard that PII/PHI. As a result, Plaintiff and hundreds of thousands of Empress' other customers ("Customers") are now the victims of a large-scale data breach that will impact them for years to come (the "Data Breach"). Specifically, the Data Breach exposed Plaintiff's and Class members' (1) name, (2) Social Security number, (3) dates of service, and (4) the name of her insurer on file with Empress.

3. Empress is responsible for allowing the Data Breach to occur because it failed to implement and maintain reasonable safeguards and failed to comply with industry-standard data security practices.

4. During the duration of the Data Breach, Empress failed to detect unauthorized third party access to Plaintiff's data, notice the massive amounts of data that were compromised, and failed to take any steps to investigate the red flags that should have warned Empress that its systems were not secure.

5. Empress had obligations created by federal law, contract, industry standards, common law, and representations made to Plaintiff and Class members to keep their PII/PHI confidential and to protect it from unauthorized access and disclosure.

6. Plaintiff and Class members provided their PII/PHI to Empress with the reasonable expectation that Empress would comply with its obligations to keep such information confidential and secure from unauthorized access.

7. Empress' data security obligations were particularly important given the substantial increase in cyberattacks and data breaches in the healthcare industry preceding the date of the Data

Breach.

8. As a result of Empress' failure to protect the consumer information it was entrusted with, Plaintiff and Class members have been exposed to and/or are at a significant risk of identity theft, financial fraud, and other identity-related fraud into the indefinite future. Plaintiff has also lost the inherent value of her PII/PHI. This harm was compounded by Empress' failure to ensure that its Customers received proper and timely notification of the Data Breach. In turn, Plaintiff and similarly situated persons suffered actual injuries in the form of loss of time as they attempted to manage the fallout from the Data Breach.

PARTIES

9. Plaintiff is a citizen and resident of the state of Florida. The conduct giving rise to Plaintiff's claims occurred in while she was attending college in New York. Plaintiff was required to provide her PII/PHI to Empress as a predicate to receiving healthcare services. On or about September 9, 2022, Plaintiff received notice from Empress that her PII/PHI had been improperly accessed and/or obtained by unauthorized third parties. This notice indicated that Plaintiff's PII/PHI, including her name, Social Security number, dates of service, and the name of her insurer on file with Empress, was compromised as a result of the Data Breach.

10. Empress is a corporation organized under the laws of the state of New York and maintains its principal place of business at 722 Nepperhan Avenue, Yonkers, New York 10703.

JURISDICTION AND VENUE

11. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. § 1332(d). The amount in controversy exceeds the sum of $5,000,000 exclusive of interest and costs, and there are more than 100 putative Class members.

12. This Court has personal jurisdiction over Empress because it is a corporation

organized under the laws of New York and has its principal place of business in Yonkers, New York.

13. Venue is proper in this District under 28 U.S.C. § 1391 because, *inter alia*, the events or omissions giving rise to the conduct alleged herein occurred in, were directed to, and/or emanated from this district; Empress' principal place of business is in this district; Empress transacts substantial business and has agents in this district; and a substantial part of the conduct giving rise to Plaintiff's claims occurred in this district.

FACTUAL ALLEGATIONS

Empress and Its Privacy and Data Security Representations

14. Founded in 1985, Empress provides 9-1-1 emergency and non-emergency medical response services for Westchester, Rockland, Ulster, Dutchess, Putnam, Orange County, and the Bronx. It has over 700 personnel, three locations, and a training center located at its headquarters in Yonkers, New York.

15. In the course of providing its services, Empress collects and maintains PII/PHI of its Customers, including their names, dates of service, insurance information, payment information, medical condition and treatment, and Social Security numbers.

16. Plaintiff was a Customer of Empress and, as a result, she provided her PHI/PHI to Empress.

17. Empress is fully aware of the sensitive nature of Customers' PII/PHI stored on or processed through its systems.

18. For example, regarding the submission of Customers' insurance information, the Billing Department page of Empress' website states: "We take your security and privacy seriously.

All your information is transferred, stored and processed safely and with discretion."[4]

19. Empress' website Privacy Policy also states, in pertinent part:

> We will not share or rent [your] information to anyone without your consent.
>
> …
>
> We will not share your information with any third party outside of our organization other than as necessary to fulfill your request.
>
> …
>
> **Security**
>
> We take precautions to protect your information. When you submit sensitive information via the website, your information is protected both online and offline.
>
> Wherever we collect sensitive information (such as credit card data), that information is encrypted and transmitted to us in a secure way. You can verify this by looking for a lock icon in the address bar and looking for "https" at the beginning of the address of the Web page.
>
> While we use encryption to protect sensitive information transmitted online, we also protect your information offline. Only employees who need the information to perform a specific job (for example, billing or customer service) are granted access to personally identifiable information. The computers/servers in which we store personally identifiable information are kept in a secure environment.[5]

20. Empress' separate Notice of Privacy Practices ("NPP") relating to Customers' submission of personal, insurance, and/or payment information also provides that Empress is "committed to protecting your personal health information" and that "[w]e respect your privacy, and treat all healthcare information about our patients with care under strict policies of confidentiality that our staff is committed to following at all times."[6]

---

[4] https://empressems.com/billing/ (last visited Oct. 6, 2022); *see also* http://web.archive.org/web/20211225191443/http://empressems.com/billing.html (last visited Oct. 7, 2022).
[5] https://empressems.com/privacy-policy/ (last visited Oct. 6, 2022).
[6] https://empressems.com/wp-content/uploads/2022/07/empressprivacy.pdf (last visited Oct. 6, 2022).

21. Empress acknowledges that it is "required by law to maintain the privacy of health information that could reasonably be used to identify you, known as 'protected health information' or 'PHI'" and that it is "also required by law to provide [Customers] with the attached detailed [NPP] explaining [its] legal duties and privacy practices with respect to [their] PHI."[7]

22. Empress' Privacy Policy and NPP are accessible through its website.

23. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class member's PII/PHI, Empress assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class members' PII/PHI from disclosure.

24. Plaintiff and Class members have taken reasonable steps to maintain the confidentiality of their PII/PHI.

25. Plaintiff and Class members relied on Empress to keep the PII/PHI of its Customers confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

Empress' Knowledge That It Was a Target of Cyber Threats

26. Empress knew it was a prime target for hackers given the significant amount of sensitive Customer PII/PHI that it collects and stores.

27. Experts studying cybersecurity routinely identify healthcare providers as being particularly vulnerable to cyberattacks because of the value of the PII and PHI which they collect and maintain.

28. Empress' knowledge is underscored by the massive number of data breaches, including those perpetrated against the healthcare sector, that have occurred in recent years.

29. Protenus, a healthcare compliance analytics firm, analyzed data breach incidents

[7] *Id.*

disclosed to the U.S. Department of Health and Human Services or the media during 2019, finding there has been an alarming increase in the number of breaches of patient privacy since 2016, when there were 450 security incidents involving patient data.[8] In 2019, that number jumped to 572 incidents, which is likely an underestimate, as two of the incidents for which there were no data affected 500 dental practices and clinics and could have affected significant volumes of patient records. Over 40 million patient records were breached in 2020.[9] In 2021, 905 health data breaches were reported.[10] Yet, according to Protenus, the impact of breaches continues to be underreported and underrepresented to the public, despite the record number of data breaches reported.[11]

30. Despite knowing the prevalence of these healthcare data breaches, Empress failed to prioritize data security by adopting reasonable data security measures to prevent and detect unauthorized access to their highly sensitive systems and databases. Empress had the resources to prevent a breach, but neglected to adequately invest in data security, despite the growing number of well-publicized data breaches affecting the healthcare industry.

31. Empress failed to undertake adequate analyses and testing of its own systems, training of its own personnel, and other data security measures to ensure that similar vulnerabilities were avoided or remedied, and that Plaintiff's and Class members' PII/PHI was protected.

---

[8] Heather Landi, *Number of Patient Records Breached Nearly Triples in 2019*, Fierce Healthcare (Feb. 20, 2020), available at https://www.fiercehealthcare.com/tech/number-patient-records-breached-2019-almost-tripledfrom-2018-as-healthcare-faces-new-threats (last visited Oct. 7, 2022); *see also* https://web.archive.org/web/20211027165416/https://www.protenus.com/resources/2020-breach-barometer (last visited Oct. 7, 2022).

[9] https://web.archive.org/web/20220301180519/https://www.protenus.com/resources/2021-breach-barometer (last accessed Oct. 7, 2022).

[10] https://www.protenus.com/breach-barometer-report (last accessed Oct. 7, 2022)

[11] *Id.*

The Data Breach

32. According to the Notice that Empress sent victims of the Data Breach, on July 14, 2022, almost two months after it began, Empress identified a network incident resulting in the encryption of some of its systems. Empress states that it took measures to contain the incident, reported it to law enforcement, and conducted a thorough investigation with the assistance of a third-party forensic firm. Empress' investigation determined that an unauthorized party first gained access to certain systems on its network on May 26, 2022, and then copied a small subset of files on July 13, 2022.[12]

33. Empress states that many of the impacted files were used by Empress for billing purposes, and its review identified documents containing Customers' name, dates of service, insurance information, and in some instances (like in Plaintiff's case), Social security numbers.[13]

34. In other words, the Notice of Data Breach concedes that PII/PHI was targeted and viewed or removed *(i.e.*, stolen) from Empress' systems.

35. Empress reported to the U.S. Department of Health and Human Services' Office of Civil Rights that approximately 318,558 individuals were affected by the Data Breach, which Empress characterized as a "Hacking/IT Incident" taking place on its network server.[14]

36. Because of the nature of the PII/PHI stored or processed by Empress, Plaintiff understands that all categories of PII/PHI were subject to unauthorized access and exfiltration, theft, or disclosure. In other words, criminals would have no purpose for hacking Empress other than to exfiltrate or steal the coveted PII/PHI stored or processed by Empress.

---

[12] https://empressems.com/notice-of-security-incident/ (last visited Oct. 6, 2022). *See also* Plaintiff's Notice of Data Breach, attached hereto as **Exhibit A**.

[13] *See id.*

[14] https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=FC0FD543A4915456A7E769BDBC7CC1DB (last visited Oct. 6, 2022).

37. Despite having knowledge of the Data Breach no later than July 14, 2022, it was not until on or about September 9, 2022 that Empress began notifying its impacted Customers, including Plaintiff, of the Data Breach.

38. Plaintiff did not receive notice of the Data Breach until approximately September 9, 2022, almost two months following Empress' alleged discovery of the Data Breach.

39. As a result of Empress' dilatory response to the Data Breach, Plaintiff and Class members have had to spend time, and will continue to spend a significant amount of time into the future, taking measures to protect themselves from identity theft, fraud, and other identity-related crimes.

40. Empress obtained and continues to maintain Plaintiff's PII/PHI and has a legal duty and obligation to protect that PII/PHI from unauthorized access and disclosure. Empress is responsible for allowing the Data Breach to occur because it failed to implement and maintain any reasonable safeguards and failed to comply with industry-standard data security practices, contrary to the representations made in various privacy statements and policies and their explicit and implied agreements with their Customers, including Plaintiff and Class members.

41. Plaintiff and Class members provided their PII/PHI to Empress with the expectation and understanding that Empress would adequately protect and store the data. Plaintiff and Class members would not have entrusted their PII/PHI to Empress had they known that it failed to maintain adequate data security.

42. Plaintiff made reasonable efforts to mitigate the Data Breach's impact after receiving the notification letter, including but not limited to reviewing her credit report, bank and credit card statements, and contacting her bank for any indications of actual or attempted identity theft or fraud. As a result, she has suffered injury. Specifically, Plaintiff has spent approximately

2 hours since the Data Breach to present dealing with issues related to the Data Breach. She will continue to expend time monitoring her credit and other identity-related information. This is valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation.

43. Empress offered twelve months of credit monitoring and identity theft protection services through Experian IdentityWorks^{SM} Credit 3B, the length of which is insufficient to protect Plaintiff's credit and identity.

44. As a result of Empress' failure to protect the sensitive PII/PHI it was entrusted with, Plaintiff and Class members are at a significant risk of identity theft, financial fraud, and other identity-related fraud into the indefinite future.

45. Plaintiff has suffered actual injury from having her PII/PHI compromised as a result of the Data Breach, including, but not limited to (a) damage to and diminution in the value of her PII/PHI, a form of property that Empress obtained from Plaintiff; (b) violation of her privacy rights; (c) imminent and impending injury arising from the increased risk of identity theft and fraud for years to come; and (d) loss of her personal time spent trying to mitigate and address harms caused by the Data Breach—time she would have spent on other matters.

46. Plaintiff has also suffered anxiety about unauthorized parties viewing, selling, and/or using her PII/PHI for purposes of identity theft and fraud. Plaintiff is extremely concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach. She is particularly concerned that she may have issues purchasing a home if her identity is stolen.

Empress Failed to Comply with Statutory and Regulatory Obligations

47. Empress had obligations created by industry standards, federal law, and common

law to keep Plaintiff and Class members' PII/PHI confidential and to protect it from unauthorized access and disclosure.

48. Empress is a covered entity and/or business associate pursuant to the Health Insurance Portability and Accountability Act ("HIPAA"), 45 C.F.R. § 160.102; accordingly, Empress must comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A through E. HIPAA's Privacy Rule ("Standards for Privacy of Individually Identifiable Health Information") establishes national standards for the protection of health information. HIPAA's Security Rule ("Security Standards for the Protection of Electronic Protected Health Information") establishes national security standards for the protection of health information that is held or transferred in electronic form. *See* 42 C.F.R. §§ 164.302-164.318.

49. HIPAA limits the permissible uses of "protected health information" and prohibits the unauthorized disclosure of "protected health information." 45 C.F.R. § 164.502. HIPAA requires that covered entities implement appropriate administrative, technical, and physical safeguards for this information and requires that covered entities reasonably safeguard protected health information from any intentional or unintentional use or disclosure that is in violation of the standards, implementation specifications or other requirements of that subpart. *See* 45 C.F.R. § 164.530(c).

50. HIPAA requires a covered entity to mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of 45 C.F.R. Part 164, Subpart E by the covered entity or its business associate. *See* 45 C.F.R. § 164.530(f).

51. Empress is a covered entity and/or business associate pursuant to the Health

Information Technology Act ("HITECH").[15] *See* 42 U.S.C. § 17921, 45 C.F.R. § 160.103.

52. HIPAA and HITECH provide guidelines for the standard of procedure dictating how patient medical information should be kept private.

53. HIPAA and HITECH obligated Empress to implement technical policies and procedures for electronic information systems that maintain electronic protected health information so that such systems were accessible only to those persons or software programs that had been granted access rights and who have a working need to access and view the information. *See* 45 C.F.R. § 164.312(a)(1); *see also* 42 U.S.C. §17902.

54. HIPAA and HITECH also obligated Empress to implement policies and procedures to prevent, detect, contain, and correct security violations, and to protect against uses or disclosures of electronic protected health information that are reasonably anticipated but not permitted by the privacy rules. *See* 45 C.F.R. § 164.306(a)(1) and § 164.306(a)(3); *see also* 42 U.S.C. §17902.

55. The Office of Civil Rights ("OCR"), within the Department of Health and Human Services ("HHS"), issues annual guidance documents on the provisions in the HIPAA Security Rule. "HHS has developed guidance and tools to assist HIPAA covered entities in identifying and implementing the most cost effective and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of e-PHI and comply with the risk analysis requirements of the Security Rule." *See* US Department of Health & Human Services, Security Rule Guidance Material.[16] The list of resources includes a link to guidelines set by the National Institute of Standards and Technology (NIST), which OCR says "represent the industry

[15] HIPAA and HITECH work together to provide guidelines and rules for maintaining protected health information. HITECH references and incorporates HIPAA.
[16] https://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html (last visited Oct. 7, 2022).

standard for good business practices with respect to standards for securing e-PHI." *See* US Department of Health & Human Services, Guidance on Risk Analysis.[17]

56. Should a health care provider experience an unauthorized disclosure, it is required to conduct a Four Factor Risk Assessment (HIPAA Omnibus Rule). This standard requires, "A covered entity or business associate must now undertake a four-factor risk assessment to determine whether or not PHI has been compromised and overcome the presumption that the breach must be reported. The four-factor risk assessment focuses on:

(1) the nature and extent of the PHI involved in the incident (*e.g.*, whether the incident involved sensitive information like social security numbers or infectious disease test results);

(2) the recipient of the PHI;

(3) whether the PHI was actually acquired or viewed; and

(4) the extent to which the risk that the PHI was compromised has been mitigated following unauthorized disclosure (*e.g.*, whether it was immediately sequestered and destroyed)."[18]

57. The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, requires HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information.

58. Empress failed to provide proper notice to Plaintiff of the disclosure and failed to conduct or improperly conducted the four-factor risk assessment following the unauthorized disclosure.

59. In addition, Empress was prohibited by the Federal Trade Commission Act ("FTC

[17] https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html (last visited Oct. 7, 2022).
[18] *See* 78 Fed. Reg. 5641-46; *see also* 45 C.F.R. § 164.304.

Act"), 15 U.S.C. § 45, from engaging in "unfair or deceptive acts or practices in or affecting commerce." The FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act.

60. Moreover, federal agencies have issued recommendations and guidelines to temper data breaches and the resulting harm to individuals and financial institutions. For example, the FTC has issued numerous guides for businesses highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[19]

61. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established guidelines for fundamental data security principles and practices for business.[20] Among other things, the guidelines note businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[21]

---

[19] *Start with Security*, A Guide for Business, FTC, https://www.ftc.gov/tips-advice/businesscenter/guidance/start-security-guide-business (last visited Oct. 7, 2022).
[20] *Protecting Personal Information: A Guide for Business, FTC*, https://www.ftc.gov/tipsadvice/business-center/guidance/protecting-personal-information-guide-business (last visited Oct. 7, 2022).
[21] *Id.*

62. Additionally, the FTC recommends that companies limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, monitor for suspicious activity on the network, and verify that third-party service providers have implemented reasonable security measures.[22]

63. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer information, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.[23]

64. Empress also failed to comply with commonly accepted industry standards for data security. Security standards commonly accepted among businesses that store PII/PHI using the internet include, without limitation:

a. Maintaining a secure firewall configuration;

b. Maintaining appropriate design, systems, and controls to limit user access to certain information as necessary;

c. Monitoring for suspicious or irregular traffic to servers;

d. Monitoring for suspicious credentials used to access servers;

e. Monitoring for suspicious or irregular activity by known users;

f. Monitoring for suspicious or unknown users;

[22] *Start with Security*, *supra* n.19.
[23] *Privacy and Security Enforcement: Press Releases, FTC*, https://www.ftc.gov/news-events/mediaresources/protecting-consumer-privacy/privacy-security-enforcement (last visited Oct. 7, 2022).

g. Monitoring for suspicious or irregular server requests;

h. Monitoring for server requests for PII;

i. Monitoring for server requests from VPNs; and

j. Monitoring for server requests from Tor exit nodes.

65. In addition to its obligations under federal law, Empress owed a duty to Plaintiff and Class members whose PII/PHI were entrusted to Empress to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII/PHI in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

66. Empress owed a duty to Plaintiff and Class members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its systems and networks adequately protected the PII/PHI of Plaintiff and Class members.

67. Empress owed a duty to Plaintiff and Class members whose PII/PHI was entrusted to Empress to design, maintain, and test its systems to ensure that the PII/PHI in Empress' possession was adequately secured and protected.

68. Empress owed a duty to Plaintiff and Class members whose PII/PHI was entrusted to Empress to create and implement reasonable data security practices and procedures to protect PII/PHI in its possession.

69. Empress owed a duty to Plaintiff and Class members whose PII/PHI was entrusted to Empress to implement processes that would detect a breach of their data security systems in a timely manner.

70. Empress owed a duty to Plaintiff and Class members whose PII/PHI was entrusted to Empress to act upon data security warnings in a timely fashion.

71. Empress owed a duty to Plaintiff and Class members whose PII/PHI was entrusted

to Empress to disclose if its systems and data security practices were inadequate to safeguard individuals' PII/PHI from theft because such an inadequacy would be a material fact in the decision to entrust PII/PHI to Empress.

72. Empress owed a duty to Plaintiff and Class members whose PII/PHI was entrusted to Empress to disclose in a timely and accurate manner when data breaches occurred.

73. Empress owed a duty of care to Plaintiff and Class members because it was a foreseeable and probable victim of any inadequacy in its affirmative development of the systems to maintain PII/PHI and in its affirmative maintenance of those systems.

74. In this case, Empress was fully aware of its obligations to use reasonable measures to protect the PII/PHI of its Customers, acknowledging as much in its various privacy statements and policies. Empress also knew it was a target for hackers. But despite understanding the consequences of inadequate data security, Empress failed to comply with industry-standard data security requirements.

75. Empress' failure to employ reasonable and appropriate measures to protect against unauthorized access to Customers' PII/PHI constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45, and N.Y. Gen. Bus. Law. § 349.

The Value of PII/PHI and Effect of the Data Breach

76. It is well known that PII/PHI is an invaluable commodity and a frequent target of hackers.

77. According to Javelin Strategy & Research, in 2017 alone over 16.7 million individuals were affected by identity theft, causing $16.8 billion to be stolen.[24]

[24] Javelin Strategy & Research, *Identity Fraud Hits All Time High With 16.7 Million U.S. Victims in 2017,* According to New Javelin Strategy & Research Study (Feb. 6, 2018), available at

78. Consumers place a high value not only on their PII/PHI, but also on the privacy of that data. This is because identity theft causes "significant negative financial impact on victims" as well as severe distress and other strong emotions and physical reactions.

79. Identity theft exacts a severe emotional toll on its victims. The 2021 Identity Theft Center survey evidences the emotional suffering experienced by victims of identity theft: 79% of respondents said their identity theft incident led them to have adverse feelings or emotions. Specifically, 84% of respondents reported feeling worried or anxious; 76% were angry; 76% felt violated; and 10% reported feeling suicidal.[25] Also, 32% of respondents said their identity crime incident led to problems with family members, and 18% reported that their identity crime incident led to problems with friends.[26]

80. Identity theft can also exact a physical toll on its victims. Another study by the Identity Theft Center found that 41% of identity theft victims experience sleep disturbances, and 29% develop other physical symptoms, including aches and pains, heart palpitations, sweating, and stomach issues.[27]

81. PII/PHI is such a valuable commodity to identity thieves that, once the information has been compromised, criminals often trade the information on the "cyber black-market" for

---

https://www.javelinstrategy.com/press-release/identity-fraud-hits-all-time-high-167-million-usvictims-2017-according-new-javelin (last visited Oct. 7, 2022).

[25] Identity Theft Resource Center, Identity Theft: The Aftermath 2017, available at https://www.idtheftcenter.org/wp-content/uploads/2021/09/ITRC_2021_Consumer_Aftermath_Report.pdf (last visited Oct. 7, 2022).

[26] *Id.*

[27] Ben Luthi, *What to Know About the Effects of Identity Theft*, Prevention (July 23, 2019), available at https://www.experian.com/blogs/ask-experian/how-long-can-the-effects-of-identity-theft-last/#:~:text=For%20example%2C%20a%20study%20by,palpitations%2C%20sweating%20and%20stomach%20issues. (last visited Oct. 7, 2022).

years. There is a strong probability that entire batches of stolen information have been dumped on the black market and will be again in the future, meaning Plaintiff and Class members are at an increased risk of fraud and identity theft for many years to come. Thus, Plaintiff and Class members must vigilantly monitor their financial and medical accounts for the foreseeable future.

82. There may be a significant time lag between when PII/PHI is stolen and when it is actually misused. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[28]

83. The risk of identity theft is particularly acute where detailed personal information is stolen, such as the PII/PHI that was compromised in the Data Breach.

84. The cyber black-market demonstrates that PII/PHI is a valuable property right.[29] Moreover, its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts, which include heavy prison sentences. This obvious risk/reward analysis illustrates that PII has considerable market value.

85. PHI is particularly valuable and has been described as a "treasure trove for criminals."[30] A cyberthief can obtain as many as "seven to ten personal identifying characteristics

---

[28] U.S. Government Accountability Office, *Report to Congressional Requesters* (June 2007), https://www.gao.gov/assets/gao-07-737.pdf (last visited Oct. 7, 2022).
[29] *See, e.g.*, John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).
[30] *See* Andrew Steager, *What Happens to Stolen Healthcare Data*, HealthTech (Oct. 20, 2019), available at https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon (last visited Oct. 7, 2022).

of an individual" from a person's PHI.[31] According to a study by Experian, the "average total cost" of medical identity theft is "about $20,000" per incident, and a majority of medical identity theft victims were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[32]

86. According to a report released by the Federal Bureau of Investigation's ("FBI") Cyber Division, criminals can sell healthcare records for 50 times the price of a stolen Social Security or credit card number.[33] Health insurance records containing sensitive health insurance information, names, addresses, telephone numbers, email addresses, SSNs, and bank account information can be sold for up to $1,200 to $1,300 each on the black market.[34]

87. Criminals can also use stolen PII/PHI to extort a financial payment by "leveraging details specific to a disease or terminal illness."[35]

88. The value of PII, including PHI, is underscored by the growing number of legitimate marketplaces allowing consumers to monetize their PII.[36]

89. As the result of Data Breach, Plaintiff and Class members have suffered or will suffer economic loss and other actual harm for which they are entitled to damages, including, but

---

[31] *Id.*
[32] *See* Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (Mar. 3, 2010), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims.
[33] Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain* (April 8, 2014), https://www.illuminweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systemscyber-intrusions.pdf.
[34] SC Staff, *Health Insurance Credentials Fetch High Prices in the Online Black Market*, SC MAGAZINE (July 16, 2013), https://www.scmagazine.com/news/breach/health-insurancecredentials-fetch-high-prices-in-the-online-black-market.
[35] *What Happens to Stolen Healthcare Data*, *supra* n.30.
[36] Markets for personal data, Project VRM, Harvard University, https://cyber.harvard.edu/projectvrm/VRM_Development_Work#Markets_for_personal_data (last visited Oct. 7, 2022).

not limited to the following:

- identity theft and fraud resulting from theft of their PII/PHI;
- costs associated with the detection and prevention of identity theft and unauthorized use of their online accounts, including financial accounts;
- losing the inherent value of their PII/PHI;
- losing the value of Empress' explicit and implicit promises of adequate data security;
- costs associated with purchasing credit monitoring and identity theft protection services;
- unauthorized access to and misuse of their online accounts;
- unauthorized charges and loss of use of and access to their financial account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit;
- lowered credit scores resulting from credit inquiries following fraudulent activities;
- costs associated with time spent and the loss of productivity or enjoyment of one's life from taking time to address and attempt to mitigate and address the actual and future consequences of the Data Breach, including discovering fraudulent charges, cancelling and reissuing cards, addressing other varied instances of identity theft – such as credit cards, bank accounts, loans, government benefits, and other services procured using the stolen PII/PHI, purchasing credit monitoring and identity theft protection services, imposing withdrawal and purchase limits on compromised accounts, and the stress, nuisance, and annoyance of dealing with the repercussions of the Data Breach;

- the continued imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII/PHI being in the possession of one or more unauthorized third parties; and
- continued risk of exposure to hackers and thieves of their PII/PHI, which remains in Empress' possession and is subject to further breaches so long as Empress fails to undertake appropriate and adequate measures to protect Plaintiff and Class members.

90. Additionally, Plaintiff and Class members place significant value in data security. According to a survey conducted by cyber-security company FireEye, approximately 50% of consumers consider data security to be a main or important consideration when making purchasing decisions and nearly the same percentage would be willing to pay more in order to work with a provider that has better data security. Likewise, 70% of consumers would provide less personal information to organizations that suffered a data breach.

91. One study on website privacy determined that U.S. consumers valued the restriction of improper access to their personal information – the very injury at issue here – between $11.33 and $16.58 per website. The study also determined that "[a]mong U.S. subjects, protection against errors, improper access, and secondary use of personal information is worth US$30.49 – 44.62." This study was done in 2002, twenty years ago. The sea-change in how pervasive the Internet is in everyday lives since then indicates that these values—when associated with the loss of PII/PHI to bad actors—would be much higher today.

92. The cost of hosting or processing Customers' PII/PHI on or through Empress' computer data and storage systems includes things such as the actual cost of the servers and employee hours needed to process said transactions. One component of the cost of using these services is the explicit and implicit promises Empress made to protect Customers' PII/PHI.

Because of the value consumers like Plaintiff and the Class members place on data privacy and security, companies with robust data security practices can command higher prices than those who do not. Indeed, if consumers did not value their data security and privacy, companies like Empress would have no reason to tout their data security efforts to their actual and potential Customers.

93. Had the victims of the Data Breach, including Plaintiff, known the truth about Empress' data security practices—that Empress would not adequately protect and store their data—they would not have entrusted PII/PHI to Empress and would not have paid for, or would have paid less for, healthcare services.

94. Plaintiff and Class members are at an imminent risk of fraud, criminal misuse of their PII/PHI, and identity theft for years to come as result of the Data Breach and Empress' deceptive and unconscionable conduct.

CLASS ACTION ALLEGATIONS

95. Pursuant to Federal Rule of Civil Procedure 23(b)(1), (b)(2) and (b)(3), Plaintiff seek certification of the following class:

> All individuals in the United States of America whose PII or PHI was compromised in the Data Breach (the "Class").

96. The Class asserts claims against Empress on behalf of the Class for negligence (Count 1), negligence per se (Count 2), declaratory judgment (Count 3), breach of express contract (Count 4), breach of implied contract (Count 5), breach of fiduciary duty (Count 6), unjust enrichment (Count 7); and violations of the New York Deceptive Acts and Practices Act, N.Y. Gen. Bus. Law § 349 ("GBL") (Count 8).

97. Excluded from the Class are Empress, any entity in which Empress has a controlling interest, and Empress' officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded from the Class are any judicial officer presiding over this

matter, members of their immediate family, members of their judicial staff, and any judge sitting in the presiding court system who may hear an appeal of any judgment entered.

98. **Risk of Inconsistent or Varying Adjudications. Fed. R. Civ. P. 23(b)(1).** While the exact number of Class members is unknown at this time, upon information and belief, there are at least hundreds of thousands of Class members; accordingly, there is significant risk of inconsistent or varying adjudications with respect to individual Class members that would establish incompatible standards of conduct for Empress. For example, injunctive relief may be entered in multiple cases, but the ordered relief may vary, causing Empress to have to choose between differing means of upgrading their data security infrastructure and choosing the court order with which it will comply. Class action status is also warranted because prosecution of separate actions by the members of the Class would create a risk of adjudications with respect to individual members of the Class that, as a practical matter, would be dispositive of the interests of other members not parties to this action, or that would substantially impair or impede their ability to protect their interests.

99. **Numerosity. Fed. R. Civ. P. 23(a)(1).** Consistent with Rule 23(a)(1), the members of the Class are so numerous and geographically dispersed that the joinder of all members is impractical. Empress has admitted that hundreds of thousands of Customers were affected by the Data Breach, and upon information and belief, there are hundreds of thousands of Class members.

100. **Commonality and Predominance. Fed. R. Civ. P. 23(a)(2) and (b)(3).** This action involves common questions of law and fact that predominate over any questions affecting individual Class members. The common questions include, but are not limited to:

a. Whether Empress unlawfully used, maintained, lost, or disclosed Plaintiff's and the Class members' PII/PHI;

b. Whether Empress failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the PII/PHI compromised in the Data Breach;

c. Whether Empress truthfully represented the nature of their security systems, including their vulnerability to hackers;

d. Whether Empress' data security programs prior to and during the Data Breach complied with applicable data security laws and regulations;

e. Whether Empress' data security programs prior to and during the Data Breach were consistent with industry standards;

f. Whether Empress owed a duty to Class members to safeguard their PII/PHI;

g. Whether Empress breached is duty to Class members to safeguard their PII/PHI;

h. Whether cyberhackers obtained, sold, copied, stored, or released Class members' PII/PHI;

i. Whether Empress knew or should have known that its data security programs and monitoring processes were deficient;

j. Whether the Class members suffered legally cognizable damages as a result of Empress' misconduct;

k. Whether Empress' conduct was negligent;

l. Whether Empress' conduct was negligent per se;

m. Whether Empress breached implied contractual duties to Plaintiff and Class members;

n. Whether Empress breached express contractual duties to Plaintiff and Class

members;

o. Whether Empress breached a fiduciary duty to Plaintiff and Class members;

p. Whether Empress was unjustly enriched by Plaintiff and Class members;

q. Whether Empress failed to provide accurate and complete notice of the Data Breach in a timely manner;

r. Whether Empress' failure to secure Plaintiff'' and Class members' PII/PHI in the manner alleged violated federal laws, state laws, or industry standards; and

s. Whether the Class members are entitled to damages, treble damages, civil penalties, punitive damages, and/or injunctive relief.

101. **Typicality. Fed. R. Civ. P. 23(a)(3).** Plaintiff's claims are typical of other Class members' claims because Plaintiff and Class members were subjected to the same allegedly unlawful conduct and damaged in the same way.

102. **Adequacy. Fed. R. Civ. P. 23(a)(4).** Consistent with Rule 23(a)(4), Plaintiff is an adequate representative of the Class. Plaintiff is a member of the Class and the Subclass. Plaintiff has no conflicts of interest with the Class. Plaintiff's counsel is competent and experienced in litigating class actions, including extensive experience in data breach and privacy litigation and consumer protection claims. Plaintiff intends to vigorously prosecute this case and will fairly and adequately protect the interests of the Class.

103. **Superiority. Fed. R. Civ. P. 23(b)(3).** Consistent with Rule 23(b)(3), a class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The purpose of the class action mechanism is to permit litigation against wrongdoers even when damages to individual plaintiffs and class members may not be sufficient to justify individual

litigation. Here, the damages suffered by Plaintiff and the Class members are relatively small compared to the burden and expense required to individually litigate their claims against Empress, and thus, individual litigation to redress Empress' wrongful conduct would be impracticable. Individual litigation by each Class member would also strain the court system. Moreover, individual litigation creates the potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court.

104. **Injunctive and Declaratory Relief. Fed. R. Civ. P. 23(b)(2).** Class certification is also appropriate under Rule 23(b)(2). Empress, through its uniform conduct, acted or refused to act on grounds generally applicable to the Class as a whole, making injunctive and declaratory relief appropriate to the Class as a whole. Moreover, Empress continues to maintain is inadequate security practices, retain possession of Plaintiff's and the Class members' PII/PHI, and has not been forced to change its practices or to relinquish PII/PHI by nature of other civil suits or government enforcement actions, thus making injunctive and declaratory relief a live issue and appropriate to the Class as a whole.

Count 1

NEGLIGENCE

105. Plaintiff repeats the allegations in paragraphs 1-104 in this Complaint, as if fully alleged herein.

106. Empress, in offering healthcare services to its Customers, knew that Plaintiff's and Class members' sensitive PII/PHI would be stored or processed by Empress' computer and data storage systems. Empress, in fact, stored and/or processed this PII/PHI through and on its computer

systems and/or databases.

107. By collecting, storing, and using this data, Empress had a duty of care to Plaintiff and Class members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting this PII/PHI in Empress' possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. More specifically, this duty included, among other things: (a) designing, maintaining, and testing Empress' security systems and data storage architecture to ensure that Plaintiff's and Class members' PII/PHI was adequately secured and protected; (b) implementing processes that would detect an unauthorized breach of Empress' security systems and data storage architecture in a timely manner; (c) timely acting on all warnings and alerts, including public information, regarding Empress' security vulnerabilities and potential compromise of the PII/PHI of Plaintiff and Class members; (d) maintaining data security measures consistent with industry standards and applicable state and federal law; and (e) timely and adequately informing Plaintiff and Class members if and when a data breach occurred notwithstanding undertaking (a) through (d) above.

108. Empress had a common law duty to prevent foreseeable harm to Plaintiff and Class members. These duties existed because Plaintiff and Class members were the foreseeable and probable victims of any inadequate security practices in Empress' affirmative collection of Customers' PII/PHI. In fact, not only was it foreseeable that Plaintiff and Class members would be harmed by the failure to protect their PII/PHI because hackers routinely attempt to steal such information and use it for nefarious purposes, but Empress also knew that more likely than not, Plaintiff and other Class members would be harmed by such theft.

109. Empress had a duty to monitor, supervise, control, or otherwise provide oversight to safeguard the PII/PHI that was collected, stored, and processed by Empress' computer and data

storage systems.

110. Empress' duties to use reasonable security measures also arose as a result of the special relationship that existed between Empress, on the one hand, and Plaintiff and Class members, on the other hand. The special relationship arose because Plaintiff and Class members entrusted Empress with PII/PHI by virtue of the healthcare services they obtained from Empress. Empress alone could have ensured that its security systems and data storage architecture were sufficient to prevent or minimize the Data Breach.

111. Empress' duty to use reasonable data security measures with regard to Plaintiff and Class members' PHI also arose under HIPAA and HITECH, as stated herein.

112. Empress' duty to use reasonable data security measures also arose under Section 5 of the FTC Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect PII. Various FTC publications and data security breach orders further form the basis of Empress' duties. In addition, individual states have enacted statutes based upon the FTC Act that also created a duty.

113. The harm that has occurred is the type of harm the HIPAA, HITECH, and FTC Act were intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of Empress' failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiff and Class members.

114. Empress knew or should have known that its computer systems and data storage architecture were vulnerable to unauthorized access and targeting by hackers for the purpose of stealing and misusing confidential PII/PHI.

115. Empress knew or should have known that a breach of its systems and data storage architecture would inflict millions of dollars of damages upon Plaintiff and the Class, and Empress was therefore charged with a duty to adequately protect this critically sensitive information.

116. Empress breached the duty it owed to Plaintiff and Class members described above and thus, was negligent. Empress breached these duties by, among other things, failing to: (a) exercise reasonable care and implement adequate security systems, protocols, and practices sufficient to protect the PII/PHI of Plaintiff and Class members; (b) detect the breach while it was ongoing; (c) maintain security systems consistent with industry standards; (d) and timely informing its Customers of the fact and extent of the Data Breach. These failures constituted violations of the HIPAA, HITECH, FTC Act, as well as a breach of duties owed to Plaintiff and Class members under the common law and New York state law.

117. Empress also failed to exercise reasonable care and breached the duty it owed Plaintiff and Class members when it provided the thieves and/or subsequent unauthorized recipients of the stolen information with additional time and cover to further purloin and re-sell the stolen PII/PHI belonging to Plaintiff and the Class members; provided the thieves and the purchasers and/or other subsequent unauthorized recipients with an opportunity to directly defraud Plaintiff and the Class; and failed to promptly notify Plaintiff and Class members of the fact that their PII/PHI was compromised and in imminent jeopardy of falling further into the hands of cyber criminals.

118. But for Empress' wrongful and negligent breach of its duties owed to Plaintiff and Class members, their PII/PHI would not have been compromised.

119. As a direct and proximate result of Empress' negligence, Plaintiff and Class members have been injured and are entitled to damages in an amount to be proven at trial. Plaintiff

has been injured, as her PII/PHI was breached as detailed herein. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII/PHI; illegal sale of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach investigating the nature of the Data Breach, reviewing bank statements, payment card statements, and credit reports; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII; lost benefit of their bargains and overcharges for services; and other economic and non-economic harm.

Count 2

NEGELIGENCE PER SE

120. Plaintiff repeats the allegations in paragraphs 1-104 in this Complaint, as if fully alleged herein, and asserts this claim in the alternative to her negligence claim to the extent necessary.

121. HIPAA and HITECH obligated Empress to implement technical policies and procedures for electronic information systems that maintain electronic protected health information so that such systems were accessible only to those persons or software programs that had been granted access rights and who have a working need to access and view the information. *See* 45 C.F.R. § 164.312(a)(1); *see also* 42 U.S.C. §17902.

122. HIPAA and HITECH also obligated Empress to implement policies and procedures to prevent, detect, contain, and correct security violations, and to protect against uses or disclosures

of electronic protected health information that are reasonably anticipated but not permitted by the privacy rules. *See* 45 C.F.R. § 164.306(a)(1) and § 164.306(a)(3); *see also* 42 U.S.C. §17902.

123. Pursuant to the FTC Act, 15 U.S.C. § 45, Empress had a duty to provide fair and adequate computer systems and data security to safeguard the PII/PHI of Plaintiff and Class members.

124. The FTC Act prohibits "unfair . . . practices in or affecting commerce," which the FTC has interpreted to include businesses' failure to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Empress' duty in this regard.

125. Empress solicited, gathered, and stored PII/PHI of Plaintiff and the Class members to facilitate transactions which affect commerce.

126. Empress violated the HIPAA, HITECH, and FTC Act by failing to use reasonable measures to protect PII/PHI of Plaintiff and the Class members and not complying with applicable industry standards, as described herein. Empress' conduct was particularly unreasonable given the nature and amount of PII/PHI obtained and stored and the foreseeable consequences of a data breach on Empress' systems.

127. Empress' violation of the HIPAA, HITECH, and FTC Act constitute negligence per se.

128. Plaintiff and the Class members are within the class of persons that the FTC Act were intended to protect. Plaintiff and Class members are also within the class of person that HIPAA and HITECH were intended to protect.

129. The harm that occurred as a result of the breach is the type of harm the FTC Act, HIPAA, and HITECH were intended to guard against.

130. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures caused the same harm as that suffered by Plaintiff and the Class members.

131. As a direct and proximate result of Empress' negligence per se, Plaintiff and the Class members have suffered, and continue to suffer, damages arising from the Data Breach as described herein and as will be proven at trial. Plaintiff has been injured, as her PII and PHI was breached as detailed herein. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII/PHI; illegal sale of the compromised PII/PHI on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach investigating the nature of the Data Breach; reviewing bank statements, payment card statements, and credit reports; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII/PHI; lost benefit of their bargains and overcharges for services; and other economic and non-economic harm.

Count 3

DECLARATORY JUDGMENT

132. Plaintiff repeats the allegations in paragraphs 1-104 in this Complaint, as if fully alleged herein.

133. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, the Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant

further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

134. An actual controversy has arisen in the wake of the Data Breach regarding Empress' present and prospective common law and other duties to reasonably safeguard its Customers' PII/PHI, and whether Empress is currently maintaining data security measures adequate to protect Plaintiff and Class members from further data breaches that compromise their PII/PHI. Plaintiff and Class members remain at imminent risk that further compromises of their PII/PHI will occur in the future. This is true even if they are not actively using Empress' services.

135. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Empress continues to owe a legal duty to secure its Customers' PII/PHI and to timely notify consumers of a data breach under the federal law, common law, and state law;

b. Empress continues to breach this legal duty by failing to employ reasonable measures to secure Plaintiff and Class members' PII/PHI.

136. The Court also should issue corresponding prospective injunctive and monetary relief pursuant to 28 U.S.C. §2202, requiring Empress to employ adequate security practices consistent with law and industry standards to protect its Customers' PII/PHI and compensate victims for the harm caused by the Data Breach.

137. If an injunction is not issued, Plaintiff and Class members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach of Empress. The risk of another such breach is real, immediate, and substantial. If another breach occurs, Plaintiff and Class members will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

138. The hardship to Plaintiff and Class members if an injunction does not issue exceeds the hardship to Empress if an injunction is issued. Among other things, if another data breach occurs at Empress, Plaintiff and Class members will likely be subjected to fraud, identify theft, and other harms described herein. On the other hand, the cost to Empress of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Empress has a pre-existing legal obligation to employ such measures.

139. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach of Empress' computer and data storage systems, thus eliminating additional injuries that would result to Plaintiff, Class members, and the hundreds of thousands of Customers of Empress whose PII/PHI would be further compromised.

Count 4

BREACH OF EXPRESS CONTRACT

140. Plaintiff repeats the allegations in paragraphs 1-104 in this Complaint, as if fully alleged herein, and asserts this claim in the alternative to her breach of implied contract claim to the extent necessary.

141. Plaintiff and Class members on the one hand and Empress on the other formed a contract pursuant to the which Plaintiff and Class members paid Empress' in exchange for its services. The clear or manifest intent of Empress to provide benefits to its Customers, including Plaintiff and Class members, through the protection of their PII/PHI that was stored or processed by Empress is evidenced by references in the Privacy Policy and NPP as set forth herein.

142. Empress' Privacy Policy provides, in pertinent part, "[t]he computers/servers in which we store personally identifiable information are kept in a secure environment."

143. The NPP further details how Empress will both protect and use the PII/PHI provided by users of Empress' services, including PII/PHI stored on or processed through Empress' databases and systems.

144. The NPP provides detailed information about what types of PII/PHI will be shared and with what entities. It further states that Empress is "committed to protecting your personal health information" and that "[w]e respect your privacy, and treat all healthcare information about our patients with care under strict policies of confidentiality that our staff is committed to following at all times."[37]

145. The NPP further specifies that it is "required by law to maintain the privacy of health information that could reasonably be used to identify you, known as [PHI]" and that it is "also required by law to provide [Customers] with the attached detailed [NPP] explaining [its] legal duties and privacy practices with respect to [their] PHI."[38]

146. Empress breached its contract with Plaintiff and Class members by failing to protect the PII/PHI. Specifically, Empress (1) failed to use reasonable measures to protect that information; (2) disclosed that information to unauthorized third parties, in violation of the agreement; and (3) failed to notify Plaintiff and Class members of the Data Breach within a reasonable time.

147. As a direct result of Empress' breach of contract, Plaintiff and the Class members have suffered injury, have been damaged as described herein and as will be proven at trial, and are entitled to damages in an amount to be proven at trial. Plaintiff has been injured, as her PII/PHI were breached as detailed herein. Such injuries include one or more of the following: ongoing,

[37] https://empressems.com/wp-content/uploads/2022/07/empressprivacy.pdf (last visited Oct. 6, 2022).
[38] *Id.*

imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII/PHI; illegal sale of the compromised PII/PHI on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach investigating the nature of the Data Breach; reviewing bank statements, payment card statements, and credit reports; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII/PHI; lost benefit of their bargains and overcharges for services; and other economic and non-economic harm.

148. All conditions precedent to bringing this claim have been performed, waived, or excused.

Count 5

BREACH OF IMPLIED CONTRACT

149. Plaintiff repeats the allegations in paragraphs 1-104 in this Complaint, as if fully alleged herein, and asserts this claim in the alternative to her breach of express contract claim to the extent necessary.

150. As consideration for the healthcare services Empress was to provide, Plaintiff provided her PII/PHI, and Class members provided their PII/PHI to Empress. When Plaintiff and Class members provided that PII/PHI to Empress, they entered into implied contracts by which Empress agreed to protect their PII/PHI and only use it under certain circumstances, including to provide healthcare services. As part of the offer, Empress would safeguard the PII/PHI using reasonable or industry standard means.

151. Accordingly, Plaintiff and the Class members accepted Empress' offer to provide healthcare services (for which Empress was compensated by Plaintiff and Class members) and provided Empress the PII/PHI. Plaintiff and Class members fully performed their obligations under the implied contracts with Empress. However, Empress breached the implied contracts by failing to safeguard Plaintiff's and Class members' PII/PHI.

152. The losses and damages Plaintiff and Class members sustained that are described herein were the direct and proximate result of Empress' breach of their implied contracts with them. Plaintiff has been injured, as her PII and PHI was breached as detailed herein. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII/PHI; illegal sale of the compromised PII/PHI on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach investigating the nature of the Data Breach; reviewing bank statements, payment card statements, and credit reports; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII/PHI; lost benefit of their bargains and overcharges for services; and other economic and non-economic harm.

153. Additionally, because Plaintiff and Class members continue to be Customers of Empress, and because damages may not provide a complete remedy for the breaches alleged herein, Plaintiff and Class members are therefore entitled to specific performance of the contracts to ensure data security measures necessary to properly effectuate the contracts maintain the security of their PII/PHI from unlawful exposure.

154. Empress' conduct as alleged herein also violated the implied covenant of good faith and fair dealing inherent in every contract, and Empress is liable to Plaintiff and Class members for associated damages and specific performance.

Count 6

BREACH OF FIDUCIARY DUTY

155. Plaintiff repeats the allegations in paragraphs 1-104 in this Complaint, as if fully alleged herein.

156. Plaintiff and Class members gave Empress, a medical provider, their PII/PHI in confidence, believing that Empress would protect that information. Plaintiff and Class members would not have provided Empress with this information had they known it would not be adequately protected. Empress' acceptance and storage of Plaintiff's and Class members' PII/PHI created a fiduciary relationship between Empress and Plaintiff and Class members. In light of this relationship, Empress must act primarily for the benefit of its patients, which includes safeguarding and protecting Plaintiff's and Class Members' PII/PHI.

157. Empress has a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of their relationship. It breached that duty by failing to properly protect the integrity of the system containing Plaintiff's and Class Members' PII/PHI, failing to comply with the data security guidelines set forth by HIPAA, and otherwise failing to safeguard Plaintiff's and Class members' PII/PHI that it collected.

158. As a direct and proximate result of Empress' breach of its fiduciary duties, Plaintiff and Class members have been injured and are entitled to damages in an amount to be proven at trial. Plaintiff has been injured, as her PII/PHI was breached as detailed herein; she has also suffered injury in the form of lost time. Such injuries include one or more of the following:

ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII/PHI; illegal sale of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach investigating the nature of the Data Breach, reviewing bank statements, payment card statements, and credit reports; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII; lost benefit of their bargains and overcharges for services; and other economic and non-economic harm.

Count 7

UNJUST ENRICHMENT

159. Plaintiff repeats the allegations in paragraphs 1-104 in this Complaint, as if fully alleged herein, and asserts this claim in the alternative to her breach of contract claim and breach of implied contract claim, to the extent necessary.

160. Plaintiff and Class members conferred a monetary benefit upon Empress in the form of monies paid for healthcare services or other services.

161. Empress accepted or had knowledge of the benefits conferred upon it by Plaintiff and Class members. Empress also benefitted from the receipt of Plaintiff's and Class members' PII/PHI, as this was used to facilitate payment. Empress will obtain said benefits without adequately compensating Plaintiff and Class members therefor.

162. As a result of Empress' conduct, Plaintiff and Class members suffered actual damages in an amount equal to the difference in value between their payments made with

reasonable data privacy and security practices and procedures that Plaintiff and Class members paid for, and those payments without reasonable data privacy and security practices and procedures that they received.

163. Empress should not be permitted to retain the money belonging to Plaintiff and Class members because Empress failed to adequately implement the data privacy and security procedures for itself that Plaintiff and Class members paid for and that were otherwise mandated by federal laws and industry standards.

164. Empress should be compelled to provide for the benefit of Plaintiff and Class members all unlawful proceeds received by it as a result of the conduct and Data Breach alleged herein.

Count 8

VIOLATIONS OF THE NEW YORK DECEPTIVE ACTS AND PRACTICES ACT

N.Y. Gen. Bus. Law § 349 ("GLB")

165. Plaintiff repeats the allegations in paragraphs 1-104 in this Complaint, as if fully alleged herein.

166. Plaintiff and Class members are "persons" within the meaning of the GBL. N.Y. Gen. Bus. Law § 349(h).

167. Empress is a "person, firm, corporation or association or agent or employee thereof" within the meaning of the GBL. N.Y. Gen. Bus. Law § 349(b).

168. Under GBL section 349, "[d]eceptive acts or practices in the conduct of any business, trade or commerce" are unlawful.

169. Empress violated the GBL through its promise to protect and subsequent failure to adequately safeguard and maintain Plaintiff and Class members' PII/PHI. Empress failed to notify

Plaintiff and other class members that, contrary to its representations about valuing data security and privacy, it does not maintain adequate controls to protect PII/PHI. It omitted all of this information from Plaintiff and class members.

170. As a result of Empress' conduct, Plaintiff and the Class have suffered damages from the disclosure of their information to unauthorized individuals.

171. As a direct and proximate result of Empress' violations of the GBL, Plaintiff and Class members have been injured and are entitled to damages in an amount to be proven at trial. Plaintiff has been injured, as her PII/PHI were breached as detailed herein. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII/PHI; illegal sale of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach investigating the nature of the Data Breach, reviewing bank statements, payment card statements, and credit reports; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII; lost benefit of their bargains and overcharges for services; and other economic and non-economic harm.

172. Plaintiff, individually and on behalf of the Class, requests that this Court enter such orders or judgments as may be necessary to enjoin Empress from continuing its unfair and deceptive practices.

173. Under the GBL, Plaintiff and Class members are entitled to recover their actual damages or $50, whichever is greater. Additionally, because Empress acted willfully or

knowingly, Plaintiff and New York Class members are entitled to recover three times their actual damages. Plaintiff also is entitled to reasonable attorneys' fees.

REQUEST FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all Class members proposed in this Complaint, respectfully requests that the Court enter judgment in her favor and against Empress as follows:

1) For an Order certifying the Class as defined herein and appointing Plaintiff and Plaintiff's counsel to represent the Class as alleged herein;

2) For injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class members;

3) For an award of compensatory, consequential, and general damages, including nominal damages, as allowed by law in an amount to be determined;

4) For an award of statutory damages and punitive damages, as allowed by law, in an amount to be determined;

5) For an award of restitution or disgorgement, in an amount to be determined;

6) For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

7) For prejudgment interest on all amounts awarded; and

8) Such other and further relief as the Court may deem just and proper.

JURY DEMAND

Plaintiff, on behalf of herself and the Class of all others similarly situated, hereby demands a trial by jury on all issues so triable pursuant to Rule 38 of the Federal Rules of Civil Procedure.

Dated: October 9, 2022

Respectfully submitted,

KOPELOWITZ OSTROW FERGUSON

WEISELBERG GILBERT

By */s/ Jason H. Alperstein*
Jason H. Alperstein (Bar No. 4904983)
Jonathan M. Streisfeld (*pro hac vice* to be filed)
Kristen Cardoso (*pro hac vice* to be filed)
1 W. Las Olas Blvd., Suite 500
Fort Lauderdale, Florida 33301
Telephone: (954) 525-4100
Facsimile: (954) 525-4300
Email: alperstein@kolawyers.com
streisfeld@kolawyers.com
cardoso@kolawyers.com

Counsel for Plaintiffs and the Proposed Classes